In the Claims

1. (original) A method for regulating access to nonvolatile digital storage contained in a device executing instructions in a Turing-complete interpreter, said method comprising:

(a) receiving a request from said instructions being executed, wherein said request specifies :

(i) a portion of said storage for which access is requested, and

(ii) a plurality of additional executable instructions;

(b) applying a cryptographic hash function to said additional executable instructions to obtain a hash value;

(c) authenticating said hash value; and

(d) provided that said authentication is successful, enabling access by said instructions being executed to said requested portion of said storage while executing said additional executable instructions.

2. (original) The method of claim 1 wherein said step of authenticating comprises comparing said hash value with a hash value stored in said nonvolatile storage.

3. (original) The method of claim 1 wherein said step of authenticating comprises verifying a digital signature provided by said instructions being executed.

4. (original) The method of claim 1 wherein said request includes a pointer to said additional executable instructions in memory accessible by said instructions being executed and contained in said device.

5. (original) A digital optical disc medium containing encrypted audiovisual content for playback on any of a plurality of device architectures, said digital optical disc medium comprising program logic configured to:

(a) identify at least one characteristic of a device executing said program logic;

(b) use said at least one characteristic to determine which, if any, of a plurality of security weaknesses are present in said executing device;

(c) when said determination indicates a suspected weakness,

(i) select at least one of a plurality of software countermeasures, wherein said selected countermeasure corresponds to said suspected weakness and is compatible with said executing device;

(ii) mitigate said suspected weakness by directing said executing device to invoke said selected countermeasure; and

(iii) decode said encrypted audiovisual content, wherein said decoding includes a result produced by successful operation of said countermeasure logic; and

(d) when said determination does not indicate a suspected weakness, decode said audiovisual content using at least one decryption key derived using at least one cryptographic key associated with said executing device.

6. (original) The digital optical disc medium of claim 5 wherein said program logic is configured to execute in an interpreter common to said plurality of device architectures, and at least a portion of said selected countermeasure is configured to be executed directly as native code on a microprocessor associated with said executing device.

7. (original) The digital optical disc medium of claim 5 wherein said digital optical disc medium further includes a digital signature authenticating said native code portion.

Please cancel claims 8-10, without prejudice.

11. (original) An automated method for determining whether to allow a portion of software stored in a computer-readable memory to access a portion of a nonvolatile memory, the method comprising:

(a) receiving a reference to said portion of software;

(b) computing a cryptographic hash of said software portion;

(c) comparing said computed cryptographic hash with a value stored in said nonvolatile memory,

(d) when said computed cryptographic hash matches said stored value, allowing said software portion to access said nonvolatile memory portion; and

(e) when said computed cryptographic hash does not match said stored value, not allowing said software portion to access said nonvolatile memory.

12. (new) The digital optical disc of claim 5 where said program logic is further adapted to cryptographically authenticate at least one of manufacturer, model, and version of the device executing said program logic.

13. (new) The digital optical disc of claim 5 where said program logic is adapted to verify as at least one characteristic of the device whether the device can perform block cipher operations using a key characteristic of at least one of manufacturer, model, and version of the device.

14. (new) The digital optical disc of claim 5 where said program logic is adapted to verify as at least one characteristic whether unauthorized firmware is present on the device.

15. (new) The digital optical disc of claim 5 where said program logic is configured to access a server over a network and to receive from the server data representing at least one of code configured to identify a new characteristic, code implementing a countermeasure, revocation status, payment information associated with content, download of bonus content, and download of advertisement.

16. (new) The digital optical disc of claim 5 where said program logic is configured to identify a characteristic by searching a portion of memory of the device.

17. (new) The digital optical disc of claim 5 where said program logic is configured to identify a characteristic by accessing non-volatile storage of the device.

18. (new) The digital optical disc of claim 5 where said program logic is further configured to make video playable by applying modifications to a video data stream.

19. (new) The digital optical disc of claim 18 where said program logic is further configured to change, when applying said modifications, audiovisual content to embed forensic information associated with playback environment.